

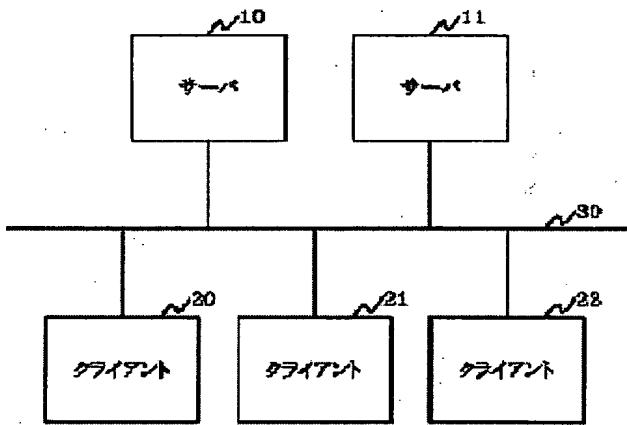
## INSTALL AND UNINSTALL CONTROLLER WITH SECURITY CHECK FUNCTION AND ITS METHOD

**Patent number:** JP2000339142  
**Publication date:** 2000-12-08  
**Inventor:** CHIBANA KAORU; YONAMINE ISAO  
**Applicant:** NEC SOFTWARE OKINAWA LTD  
**Classification:**  
- International: G06F9/06  
- european:  
**Application number:** JP19990149440 19990528  
**Priority number(s):**

### Abstract of JP2000339142

**PROBLEM TO BE SOLVED:** To prevent a misoperation due to any malicious illegal operation or a fault, and to further safely realize the install and uninstall of an application by checking the security of an executer at the time of operating the install and uninstall of the application.

**SOLUTION:** This device is composed of a sever 10 which security-checks whether or not a request for the permission of the install and uninstall of an application is proper, a server 11 which substitutes for the server 10 when the server 10 breaks down, clients 20, 21, and 22 which request the permission of the install and uninstall of the application, a storage device 100 which stores data necessary for the processing of the server, and a network cable 30 for connecting each server 10 and 11 with each client 20-22.



Data supplied from the **esp@cenet** database - Worldwide

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-339142

(P 2 0 0 0 - 3 3 9 1 4 2 A)

(43) 公開日 平成12年12月8日 (2000.12.8)

マークド (参考)

(51) Int. Cl. 7  
G 06 F 9/06

識別記号  
410  
550

F I  
G 06 F 9/06 410 B 5B076  
550 Z

審査請求 有 請求項の数15 OL (全 14 頁)

(21) 出願番号 特願平11-149440  
(22) 出願日 平成11年5月28日 (1999.5.28)

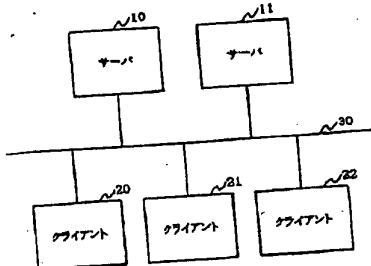
(71) 出願人 000123262  
沖縄日本電気ソフトウェア株式会社  
沖縄県那覇市久米2丁目3番15号  
(72) 発明者 知花 薫  
沖縄県那覇市久米2丁目3番15号 沖縄日本  
電気ソフトウェア株式会社内  
(72) 発明者 與那嶺 熱  
沖縄県那覇市久米2丁目3番15号 沖縄日本  
電気ソフトウェア株式会社内  
(74) 代理人 100082935  
弁理士 京本 直樹 (外2名)  
F ターム (参考) 5B076 AA01 AA11 FA06 FB11

(54) 【発明の名称】セキュリティチェック機能付きインストール及びアンインストール制御装置と方法

(57) 【要約】

【課題】実行者のセキュリティがチェックされないために、誰もがアプリケーションのインストール及びアンインストールを実行できてしまう。

【解決手段】アプリケーションのインストール及びアンインストールの許可要求が妥当かどうかをセキュリティインストールの代理を行うサーバ10、サーバ11、アプリケーションのインストール及びアンインストールの許可要求をするクライアント20、21、22、サーバの処理に必要なデータを蓄積している記憶装置100、及び各サーバと各クライアントを結ぶネットワークケーブル30から構成し、アプリケーションのインストール及びアンインストールにおいて実行者のセキュリティをチェックすることにより、悪意を持った不正操作や過失による誤操作を防ぎ、より安全にアプリケーションのインストール及びアンインストールを行う。



### 【特許請求の範囲】

【特許請求の範囲】  
【請求項1】 アプリケーションのインストール及びアンインストールをクライアントで実行時、アプリケーションのインストール及びアンインストール開始状態であることをクライアントのオペレーティングシステムが検知し、アプリケーションのインストール及びアンインストールを一時停止状態した後サーバへアプリケーションのインストール及びアンインストールの許可要求し、サーバは各クライアントからの許可要求が妥当なものかどうか許可要求と同時に送られたログオンユーザ名及びパスワードの含まれた許可要求データを元にセキュリティチェックを行い、正常な操作が行われた場合は、サーバはアプリケーションのインストール及びアンインストールの許可要求が妥当であるとセキュリティチェックで判断し、各クライアントへ実行許可を通知し、各クライアントは通知を受け取った後、アプリケーションのインストール及びアンインストールを継続し、悪意を持った不正操作や過失による誤操作が行われた場合は、サーバはアプリケーションのインストール及びアンインストールの許可要求が妥当でないとセキュリティチェックで判断し、各クライアントへ実行拒否を通知し、各クライアントでは通知を受け取った後、アプリケーションのインストール及びアンインストールを中止することを特徴とするセキュリティチェック機能付きインストール及びアンインストール制御装置。

【請求項2】 アプリケーションのインストール及びアンインストールの許可要求が妥当かどうかをセキュリティチェックするサーバと、アプリケーションのインストール及びアンインストールの許可要求をするクライアントと、クライアントとサーバの処理に必要なデータを蓄積している記憶装置と、サーバと各クライアントを結ぶネットワークケーブルから構成し、サーバは、クライアントから送信された許可要求データを処理するデータ生成部と、データ制御部、データ検証部を備え、データ生成部は、復号生成部、暗号生成部、認証生成部からなり、復号生成部は、暗号化されたデータをデータ検証部で処理できるように復号化し、暗号生成部は、復号化されたデータを記憶装置で保管できるように暗号化し、認証生成部は、復号生成部で復号化されたデータからデータ検証部で検証するためのデータを生成し、データ制御部は、クライアント、データ生成部、データ制御部、データ検証部、記憶装置を行き交うデータの流れを制御し、データ検証部は、クライアントより送られた許可要求データが妥当なものであるかを検証することを特徴とするセキュリティチェック機能付きインストール及びアンインストール制御装置。

【請求項3】 クライアントでアプリケーションのインストール及びアンインストールの実行が開始されると、クライアントのオペレーティングシステムがアプリケーションのインストール及びアンインストール開始状態を

検知し、クライアントのオペレーティングシステムでアプリケーションのインストール及びアンインストールを一時停止状態にし、クライアントで現在操作している実行者のデータを暗号化し、アプリケーションのインストール及びアンインストール許可を要求する許可要求データとしてサーバへ送信し、サーバは、クライアントから送信された許可要求データをデータ制御部で受信し、データ制御部は、許可要求データをデータ生成部の復号生成部へ送り、復号生成部は、許可要求データを復号化しデータ制御部を介してデータ検証部へ送り、データ制御部は、記憶装置に格納されているインデックスデータを取り出し、データ生成部の復号生成部へ送り、復号生成部は、インデックスデータを復号化し、データ制御部を介してデータ検証部へ送り、データ検証部は、許可要求データのクライアントマシン名がネットワークに存在するもののかをサーバのオペレーティングシステムに問い合わせ、存在するならば、許可要求データのログオンユーザ名またはパスワードと、インデックスデータのログオンユーザ名またはパスワードが一致するものを検索し、同じデータが見つかった場合は、データ制御部がインデックスデータのナンバーをキーとして、記憶装置に格納されている認証データを取り出し、データ生成部の復号生成部へ送り、復号生成部は、認証データを復号化し、データ制御部を介してデータ検証部へ送り、データ検証部では、許可要求データのアプリケーション名、アプリケーションのバージョン情報と、認証データのアプリケーション名、アプリケーションのバージョン情報が一致するものを検索し、同じデータが見つかった場合は、アプリケーションのインストール及びアンインストールの実行権限情報が実行可能になっているかをチェックし、アプリケーションのインストール及びアンインストール許可の要求が不正なものでないか判断し、不正な要求でない正当なアプリケーションのインストール及びアンインストール許可の要求であった場合は、認証データをデータ生成の認証生成部へ送り、認証生成部は、認証データに正常な操作である旨の正常操作、クライアントマシン名、ログオンユーザ名、パスワード、操作が行われた時間を含む履歴情報を付加し、履歴情報を付加された認証データは、データ制御部を介してデータ生成部へ送り、暗号化し、暗号化された認証データはデータ制御部を介して記憶装置へ保管し、データ制御部は認証データが保管された後に、クライアントへアプリケーションのインストール及びアンインストール許可を通知する許可または拒否通知データを送信し、クライアントはサーバより送られたアプリケーションのインストール及びアンインストール許可を通知する許可または拒否通知データを受信し、アプリケーションのインストール及びアンインストールを継続すること、また、悪意を持った不正操作や過失による誤操作が行われた場合は、ネットワークに存在しないクライアントマシン名か

3

らの不正操作、ログオンユーザ名またはパスワードが不正であることを検出可能にし、個々のアプリケーションに対して不正なインストール及びアンインストールが要求されたかを検出し、検出されたら認証データをデータ生成部へ送り、認証生成部は、認証データに生成の認証生成部へ送り、認証生成部は、認証データに不正な操作である旨の不正操作の原因究明に必要なデータの異常操作、クライアントマシン名、ログオンユーザ名、パスワード、操作が行われた時間を含む履歴情報を付加し、履歴が付加された認証データは、データ制御部を介してデータ生成部の暗号生成部へ送り暗号化し、暗号化された認証データは、データ制御部を介して記憶装置へ保管し、データ制御部は認証データデータが保管された後に、クライアントへアプリケーションのインストール及びアンインストール拒否を通知する許可または拒否通知データを送信し、クライアントではサーバより送られたアプリケーションのインストール及びアンインストール拒否を通知する許可または拒否通知データを受信し、アプリケーションのインストール及びアンインストールを中止して終了することを特徴とするセキュリティチェック機能付きインストール及びアンインストール制御装置。

【請求項4】 处理装置は入力装置と出力装置を備え、オペレーティングシステムがアプリケーションのインストール及びアンインストールの開始を検知すると、出力装置にキーワード入力画面を表示し、実行者に対して、入力装置よりキーワードを入力させ、マシン名、ユーザ名、パスワード、及びキーワードを含む実行者のデータ名を作成し、アプリケーションのインストール及びアンインストール許可を要求する許可要求データとして、データ制御部を介してデータ検証部へ送り、同時にデータ制御部は、記憶装置に格納されているインデックスデータを取り出し、データ生成部の復号生成部へ送り、復号生成部は、インデックスデータを復号化し、データ制御部を介してデータ検証部へ送り、データ検証部は、許可要求データとインデックスデータを比較し、許可要求データが不正なものでないかを判断し、正常な要求の場合、アプリケーションのインストール及びアンインストールの許可通知データを作成し、アプリケーションのインストール及びアンインストール処理を継続する、また、要求データが不正なものであった場合は、アプリケーションのインストール及びアンインストール不許可通知である拒否通知データを作成し、出力装置にアプリケーションのインストール及びアンインストールの拒否を示すメッセージを表示し、アプリケーションのインストール及びアンインストール処理を終了させることを特徴とするセキュリティチェック機能付きインストール及びアンインストール制御装置。

【請求項5】 处理装置は入力装置と出力装置を備え、ファイルの作成及び削除を検知すると、出力装置にキーワード入力画面を表示して、実行者に対して、入力装置

4

よりキーワードを入力させ、マシン名、ユーザ名、パスワード、及びキーワードを含む実行者のデータを暗号化して、ファイルの作成及び削除許可を要求する許可要求データを作成し、また、ファイルの作成及び削除拒否通知データを作成した場合は、出力装置にファイルの作成及び削除の拒否を示すメッセージを表示し、ファイルの作成及び削除処理を終了することを特徴とするセキュリティチェック機能付きインストール及びアンインストール制御装置。

【請求項6】 アプリケーションのインストール及びアンインストールをクライアントで実行時、アプリケーションのインストール及びアンインストール開始状態であることをクライアントのオペレーティングシステムが検知し、アプリケーションのインストール及びアンインストールを一時停止状態した後サーバへアプリケーションのインストール及びアンインストールの許可要求し、サーバは各クライアントからの許可要求が妥当なものかどうかを許可要求と同時に送られたログオンユーザ名及びパスワードの含まれた許可要求データを元にセキュリティチェックを行い、正常な操作が行われた場合は、サーバはアプリケーションのインストール及びアンインストールの許可要求が妥当であるとセキュリティチェックで判断し、各クライアントへ実行許可を通知し、各クライアントは通知を受け取った後、アプリケーションのインストール及びアンインストールを継続し、悪意を持った不正操作や過失による誤操作が行われた場合は、サーバはアプリケーションのインストール及びアンインストールの許可要求が妥当でないとセキュリティチェックで判断し、各クライアントへ実行拒否を通知し、各クライアントでは通知を受け取った後、アプリケーションのインストール及びアンインストールを中止することを特徴とするセキュリティチェック機能付きインストール及びアンインストール制御方法。

【請求項7】 アプリケーションのインストール及びアンインストールの許可要求が妥当かどうかをセキュリティチェックするサーバと、アプリケーションのインストール及びアンインストールの許可要求をするクライアントと、クライアントとサーバの処理に必要なデータを蓄積している記憶装置と、サーバと各クライアントを結ぶネットワークケーブルから構成し、サーバは、クライアントから送信された許可要求データを処理するデータ生成部と、データ制御部、データ検証部を備え、データ生成部は、復号生成部、暗号生成部、認証生成部からなり、復号生成部は、暗号化されたデータをデータ検証部で処理できるように復号化し、暗号生成部は、復号化されたデータを記憶装置で保管できるように暗号化し、認証生成部は、復号生成部で復号化されたデータからデータ検証部で検証するためのデータを生成し、データ制御部は、クライアント、データ生成部、データ制御部、データ検証部、記憶装置を行き交うデータの流れを制御

し、データ検証部は、クライアントより送られた許可要求データが妥当なものであるかを検証することを特徴とするセキュリティチェック機能付きインストール及びアンインストール制御方法。

【請求項8】 クライアントでアプリケーションのインストール及びアンインストールの実行が開始されると、クライアントのオペレーティングシステムがアプリケーションのインストール及びアンインストール開始状態を検知し、クライアントのオペレーティングシステムでアプリケーションのインストール及びアンインストールを一時停止状態にし、クライアントで現在操作している実行者のデータを暗号化し、アプリケーションのインストール及びアンインストール許可を要求する許可要求データとしてサーバへ送信し、サーバは、クライアントから送信された許可要求データをデータ制御部で受信し、データ制御部は、許可要求データをデータ生成部の復号生成部へ送り、復号生成部は、許可要求データを復号化しデータ制御部を介してデータ検証部へ送り、データ制御部は、記憶装置に格納されているインデックスデータを取り出し、データ生成部の復号生成部へ送り、復号生成部は、インデックスデータを復号化し、データ制御部を介してデータ検証部へ送り、データ検証部は、許可要求データのクライアントマシン名がネットワークに存在するもののかをサーバのオペレーティングシステムに問い合わせ、存在するならば、許可要求データのログオンユーザ名またはパスワードと、インデックスデータのログオンユーザ名またはパスワードが一致するものを検索し、同じデータが見つかった場合は、データ制御部がインデックスデータのナンバーをキーとして、記憶装置に格納されている認証データを取り出し、データ生成部の復号生成部へ送り、復号生成部は、認証データを復号化し、データ制御部を介してデータ検証部へ送り、データ検証部では、許可要求データのアプリケーション名、アプリケーションのバーション情報と、認証データのアプリケーション名、アプリケーションのバーション情報が一致するものを検索し、同じデータが見つかった場合は、アプリケーションのインストール及びアンインストールの実行権限情報が実行可能になっているかをチェックし、アプリケーションのインストール及びアンインストール許可の要求が不正なものでないか判断し、不正なインストール許可の要求であった場合は、認証データをデータ生成の認証生成部へ送り、認証生成部は、認証データに正常な操作である旨の正常操作、クライアントマシン名、ログオンユーザ名、パスワード、操作が行われた時間を含む履歴情報を付加し、履歴情報を付加された認証データは、データ制御部を介してデータ生成部へ送り、暗号化し、暗号化された認証データはデータ制御部を介して記憶装置へ保管し、データ制御部は認証データが保管された後に、クライアントへ

6  
プリケーションのインストール及びアンインストール許可を通知する許可または拒否通知データを送信し、クライアントはサーバより送られたアプリケーションのインストール及びアンインストール許可を通知する許可または拒否通知データを受信し、アプリケーションのインストール及びアンインストールを継続すること、また、悪意を持った不正操作や過失による誤操作が行われた場合は、ネットワークに存在しないクライアントマシン名からの不正操作、ログオンユーザ名またはパスワードが不正であることを検出可能にし、個々のアプリケーションに対して不正なインストール及びアンインストールが要求されたかを検出し、検出されたら認証データをデータ生成の認証生成部へ送り、認証生成部は、認証データに不正な操作である旨の不正操作の原因究明に必要なデータの異常操作、クライアントマシン名、ログオンユーザ名、パスワード、操作が行われた時間を含む履歴情報を付加し、履歴が付加された認証データは、データ制御部を介してデータ生成部の暗号生成部へ送り暗号化し、暗号化された認証データは、データ制御部を介して記憶装置へ保管し、データ制御部は認証データデータが保管された後に、クライアントへアプリケーションのインストール及びアンインストール拒否を通知する許可または拒否通知データを送信し、クライアントではサーバより送られたアプリケーションのインストール及びアンインストール拒否を通知する許可または拒否通知データを受信し、アプリケーションのインストール及びアンインストールを中止して終了することを特徴とするセキュリティチェック機能付きインストール及びアンインストール制御方法。

【請求項9】 処理装置は入力装置と出力装置を備え、オペレーティングシステムがアプリケーションのインストール及びアンインストールの開始を検知すると、出力装置にキーワード入力画面を表示し、実行者に対して、入力装置よりキーワードを入力させ、マシン名、ユーザ名、パスワード、及びキーワードを含む実行者のデータを作成し、アプリケーションのインストール及びアンインストール許可を要求する許可要求データとして、データ制御部を介してデータ検証部へ送り、同時にデータ制御部は、記憶装置に格納されているインデックスデータを取り出し、データ生成部の復号生成部へ送り、復号生成部は、インデックスデータを復号化し、データ制御部を介してデータ検証部へ送り、データ検証部は、許可要求データとインデックスデータを比較し、許可要求データが不正なものでないかを判断し、正常な要求の場合は、アプリケーションのインストール及びアンインストールの許可通知データを作成し、アプリケーションのインストール及びアンインストール処理を継続する、また、要求データが不正なものであった場合は、アプリケーションのインストール及びアンインストール不許可通知である拒否通知データを作成し、出力装置にアプリケ

ーションのインストール及びアンインストールの拒否を示すメッセージを表示し、アプリケーションのインストール及びアンインストール処理を終了させることを特徴とするセキュリティチェック機能付きインストール及びアンインストール制御方法。

【請求項10】 处理装置は入力装置と出力装置を備え、ファイルの作成及び削除を検知すると、出力装置にキーワード入力画面を表示して、実行者に対して、入力装置よりキーワードを入力させ、マシン名、ユーザ名、パスワード、及びキーワードを含む実行者のデータを暗号化して、ファイルの作成及び削除許可を要求する許可要求データを作成し、また、ファイルの作成及び削除拒否通知データを作成した場合は、出力装置にファイルの作成及び削除の拒否を示すメッセージを表示し、ファイルの作成及び削除処理を終了することを特徴とするセキュリティチェック機能付きインストール及びアンインストール制御方法。

【請求項11】 アプリケーションのインストール及びアンインストールをクライアントで実行時、アプリケーションのインストール及びアンインストール開始状態であることをクライアントのオペレーティングシステムが検知し、アプリケーションのインストール及びアンインストールを一時停止状態した後サーバへアプリケーションのインストール及びアンインストールの許可要求し、サーバは各クライアントからの許可要求が妥当なものかどうか許可要求と同時に送られたログオンユーザ名及びパスワードの含まれた許可要求データを元にセキュリティチェックを行い、正常な操作が行われた場合は、サーバはアプリケーションのインストール及びアンインストールの許可要求が妥当であるとセキュリティチェックで判断し、各クライアントへ実行許可を通知し、各クライアントは通知を受け取った後、アプリケーションのインストール及びアンインストールを継続し、悪意を持った不正操作や過失による誤操作が行われた場合は、サーバはアプリケーションのインストール及びアンインストールの許可要求が妥当でないとセキュリティチェックで判断し、各クライアントへ実行拒否を通知し、各クライアントでは通知を受け取った後、アプリケーションのインストール及びアンインストールを中止する処理をコンピュータに実行させるためのプログラムを記録したことを特徴とする記録媒体。

【請求項12】 アプリケーションのインストール及びアンインストールの許可要求が妥当かどうかをセキュリティチェックするサーバと、アプリケーションのインストール及びアンインストールの許可要求をするクライアントと、クライアントとサーバの処理に必要なデータを蓄積している記憶装置と、サーバと各クライアントを結ぶネットワークケーブルから構成し、サーバは、クライアントから送信された許可要求データを処理するデータ生成部と、データ制御部、データ検証部を備え、データ

生成部は、復号生成部、暗号生成部、認証生成部からなり、復号生成部は、暗号化されたデータをデータ検証部で処理できるように復号化し、暗号生成部は、復号化されたデータを記憶装置で保管できるように暗号化し、認証生成部は、復号生成部で復号化されたデータからデータ検証部で検証するためのデータを生成し、データ制御部は、クライアント、データ生成部、データ制御部、データ検証部、記憶装置を行き交うデータの流れを制御し、データ検証部は、クライアントより送られた許可要求データが妥当なものであるかを検証する処理をコンピュータに実行させるためのプログラムを記録したことを特徴とする記録媒体。

【請求項13】 クライアントでアプリケーションのインストール及びアンインストールの実行が開始されると、クライアントのオペレーティングシステムがアプリケーションのインストール及びアンインストール開始状態を検知し、クライアントのオペレーティングシステムでアプリケーションのインストール及びアンインストールを一時停止状態にし、クライアントで現在操作している実行者のデータを暗号化し、アプリケーションのインストール及びアンインストール許可を要求する許可要求データとしてサーバへ送信し、サーバは、クライアントから送信された許可要求データをデータ制御部で受信し、データ制御部は、許可要求データをデータ生成部の復号生成部へ送り、復号生成部は、許可要求データを復号化しデータ制御部を介してデータ検証部へ送り、データ制御部は、記憶装置に格納されているインデックスデータを取り出し、データ生成部の復号生成部へ送り、復号生成部は、インデックスデータを復号化し、データ制御部を介してデータ検証部へ送り、データ検証部は、許可要求データのクライアントマシン名がネットワークに存在するもののかをサーバのオペレーティングシステムに問い合わせ、存在するならば、許可要求データのログオンユーザ名またはパスワードと、インデックスデータのログオンユーザ名またはパスワードが一致するものを検索し、同じデータが見つかった場合は、データ制御部がインデックスデータのナンバーをキーとして、記憶装置に格納されている認証データを取り出し、データ生成部の復号生成部へ送り、復号生成部は、認証データを復号化し、データ制御部を介してデータ検証部へ送り、データ検証部では、許可要求データのアプリケーション名、アプリケーションのバージョン情報と、認証データのアプリケーション名、アプリケーションのバージョン情報が一致するものを検索し、同じデータが見つかった場合は、アプリケーションのインストール及びアンインストールの実行権限情報が実行可能になっているかをチェックし、アプリケーションのインストール及びアンインストール許可の要求が不正なものでないか判断し、不正な要求でない正当なアプリケーションのインストール及びアンインストール許可の要求であった場合は、認証

データをデータ生成の認証生成部へ送り、認証生成部は、認証データに正常な操作である旨の正常操作、クライアントマシン名、ログオンユーザ名、パスワード、操作が行われた時間を含む履歴情報を付加し、履歴情報を付加された認証データは、データ制御部を介してデータ生成部の暗号生成部へ送り、暗号化し、暗号化された認証データはデータ制御部を介して記憶装置へ保管し、データ制御部は認証データが保管された後に、クライアントへアプリケーションのインストール及びアンインストール許可を通知する許可または拒否通知データを送信し、クライアントはサーバより送られたアプリケーションのインストール及びアンインストール許可を通知する許可または拒否通知データを受信し、アプリケーションのインストール及びアンインストールを継続すること、また、悪意を持った不正操作や過失による誤操作が行われた場合は、ネットワークに存在しないクライアントマシン名からの不正操作、ログオンユーザ名またはパスワードが不正であることを検出可能にし、個々のアプリケーションに対して不正なインストール及びアンインストールが要求されたかを検出し、検出されたら認証データをデータ生成の認証生成部へ送り、認証生成部は、認証データに不正な操作である旨の不正操作の原因究明に必要なデータの異常操作、クライアントマシン名、ログオンユーザ名、パスワード、操作が行われた時間を含む履歴情報を付加し、履歴が付加された認証データは、データ制御部を介してデータ生成部の暗号生成部へ送り暗号化し、暗号化された認証データは、データ制御部を介して記憶装置へ保管し、データ制御部は認証データデータが保管された後に、クライアントへアプリケーションのインストール及びアンインストール拒否を通知する許可または拒否通知データを送信し、クライアントではサーバより送られたアプリケーションのインストール及びアンインストール拒否を通知する許可または拒否通知データを受信し、アプリケーションのインストール及びアンインストールを中止して終了する処理をコンピュータに実行させるためのプログラムを記録したことを特徴とする記録媒体。

【請求項14】 处理装置は入力装置と出力装置を備え、オペレーティングシステムがアプリケーションのインストール及びアンインストールの開始を検知すると、出力装置にキーワード入力画面を表示し、実行者に対して、入力装置よりキーワードを入力させ、マシン名、ユーザ名、パスワード、及びキーワードを含む実行者のデータを作成し、アプリケーションのインストール及びアンインストール許可を要求する許可要求データとして、データ制御部を介してデータ検証部へ送り、同時にデータ制御部は、記憶装置に格納されているインデックスデータ制御部は、記憶装置に格納されているインデックスデータを取り出し、データ生成部の復号生成部へ送り、復号生成部は、インデックスデータを復号化し、データ制御部を介してデータ検証部へ送り、データ検証部は、許

可要求データとインデックスデータを比較し、許可要求データが不正なものでないかを判断し、正常な要求の場合は、アプリケーションのインストール及びアンインストールの許可通知データを作成し、アプリケーションのインストール及びアンインストール処理を継続する、また、要求データが不正なものであった場合は、アプリケーションのインストール及びアンインストール不許可通知である拒否通知データを作成し、出力装置にアプリケーションのインストール及びアンインストールの拒否を示すメッセージを表示し、アプリケーションのインストール及びアンインストール処理を終了させる処理をコンピュータに実行させるためのプログラムを記録したこと

を特徴とする記録媒体。

【請求項15】 处理装置は入力装置と出力装置を備え、ファイルの作成及び削除を検知すると、出力装置にキーワード入力画面を表示して、実行者に対して、入力装置よりキーワードを入力させ、マシン名、ユーザ名、パスワード、及びキーワードを含む実行者のデータを暗号化して、ファイルの作成及び削除許可を要求する許可要求データを作成し、また、ファイルの作成及び削除拒否通知データを作成した場合は、出力装置にファイルの作成及び削除の拒否を示すメッセージを表示し、ファイルの作成及び削除処理を終了する処理をコンピュータに実行させるためのプログラムを記録したことを特徴とする記録媒体。

#### 【発明の詳細な説明】

##### 【0001】

【発明の属する技術分野】 本発明はセキュリティチェック機能付きインストール及びアンインストール制御装置と方法に関し、特にアプリケーションのインストール及びアンインストールにおいて実行者のセキュリティをチェックすることにより、より安全にアプリケーションのインストール及びアンインストールを行うセキュリティチェック機能付きインストール及びアンインストール制御装置と方法に関する。

##### 【0002】

【従来の技術】 従来、アプリケーションのインストール及びアンインストールにおいてのセキュリティチェックは、アプリケーションのCD-ROMやマニュアルに記載されているIDを入力することで、インストール及びアンインストールプログラムがIDチェックを行っていた。

##### 【0003】

【発明が解決しようとする課題】 上述した従来のセキュリティチェック機能付きインストール及びアンインストールは、第1の問題点は、アプリケーションのインストール及びアンインストールを実行する実行者のセキュリティがチェックされないために、誰もがアプリケーションのインストール及びアンインストールを実行できることがある。

11  
【0004】その理由は、従来のアプリケーションのインストール及びアンインストールでは実行者のセキュリティチェックは考慮されていないためである。

【0005】本発明の目的は、アプリケーションのインストール及びアンインストールにおいて実行者のセキュリティをチェックすることにより、悪意を持った不正操作や過失による誤操作を防ぎ、より安全にアプリケーションのインストール及びアンインストールを行うことができるセキュリティチェック機能付きインストール及びアンインストール制御装置と方法を提供するものである。

【0006】

【課題を解決するための手段】第1の発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法は、クライアントでアプリケーションのインストール及びアンインストールの実行が開始されたと、クライアントのオペレーティングシステムがアプリケーションのインストール及びアンインストール開始状態を検知し、クライアントのオペレーティングシステムでアプリケーションのインストール及びアンインストールを一時停止状態にし、クライアントで現在操作している実行者のデータを暗号化し、アプリケーションのインストール及びアンインストール許可を要求する許可要求データとしてサーバへ送信し、サーバは、クライアントから送信された許可要求データをデータ制御部で受信し、データ制御部は、許可要求データをデータ生成部の復号生成部へ送り、復号生成部は、許可要求データを復号化しデータ制御部を介してデータ検証部へ送り、データ制御部は、記憶装置に格納されているインデックスデータを取り出し、データ生成部の復号生成部へ送り、復号生成部は、インデックスデータを復号化し、データ制御部を介してデータ検証部へ送り、データ検証部は、許可要求データのクライアントマシン名がネットワークに存在するもののかをサーバのオペレーティングシステムに問い合わせ、存在するならば、許可要求データのロゴオンユーザ名またはパスワードと、インデックスデータのロゴオンユーザ名またはパスワードが一致するもののログオンユーザ名またはパスワードが一致する場合は、データ制御部がインデックスデータのナンバーをキーとして、記憶装置に格納されている認証データを取り出し、データ生成部の復号生成部へ送り、復号生成部は、認証データを復号化し、データ制御部を介してデータ検証部へ送り、データ検証部では、許可要求データのアプリケーション名、アプリケーションのバージョン情報と、認証データのアプリケーション名、アプリケーションのバージョンの情報を一致するものを検索し、同じデータが見つかった場合は、アプリケーションのインストール及びアンインストールの実行権限情報を実行可能になっているかをチェックし、アプリケーションのインストール及びアンインストール許可の要求が不正なものでないか判断し、不

正な要求でない正当なアプリケーションのインストール及びアンインストール許可の要求であった場合は、認証データをデータ生成の認証生成部へ送り、認証生成部は、認証データに正常な操作である旨の正常操作、クライアントマシン名、ログオンユーザ名、パスワード、操作が行われた時間を含む履歴情報を付加し、履歴情報を付加された認証データは、データ制御部を介してデータ生成部へ送り、暗号化し、暗号化された認証データはデータ制御部を介して記憶装置へ保管し、データ制御部は認証データが保管された後に、クライアントへアプリケーションのインストール及びアンインストール許可を通知する許可または拒否通知データを送信し、クライアントはサーバより送られたアプリケーションのインストール及びアンインストール許可を通知する許可または拒否通知データを受信し、アプリケーションのインストール及びアンインストールを継続すること、また、悪意を持った不正操作や過失による誤操作が行われた場合は、ネットワークに存在しないクライアントマシン名からの不正操作、ログオンユーザ名またはパスワードが不正であることを検出可能にし、個々のアプリケーションに対して不正なインストール及びアンインストールが要求されたかを検出し、検出されたら認証データをデータ生成の認証生成部へ送り、認証生成部は、認証データに不正な操作である旨の不正操作の原因究明に必要なデータの異常操作、クライアントマシン名、ログオンユーザ名、パスワード、操作が行われた時間を含む履歴情報を付加し、履歴が付加された認証データは、データ制御部を介してデータ生成部の暗号生成部へ送り暗号化し、暗号化された認証データは、データ制御部を介して記憶装置へ保管し、データ制御部は認証データデータが保管された後に、クライアントへアプリケーションのインストール及びアンインストール拒否を通知する許可または拒否通知データを送信し、クライアントではサーバより送られたアプリケーションのインストール及びアンインストール拒否を通知する許可または拒否通知データを受信し、アプリケーションのインストール及びアンインストールを中止して終了するように構成されている。

【0007】また、第2の発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法は、処理装置は入力装置と出力装置を備え、オペレーティングシステムがアプリケーションのインストール及びアンインストールの開始を検知すると、出力装置にキーワード入力画面を表示し、実行者に対して、入力装置よりキーワードを入力させ、マシン名、ユーザ名、パスワード、及びキーワードを含む実行者のデータを作成し、アプリケーションのインストール及びアンインストール許可を要求する許可要求データとして、データ制御部を介してデータ検証部へ送り、同時にデータ制御部は、記憶装置に格納されているインデックスデータを取

り出し、データ生成部の復号生成部へ送り、復号生成部は、インデックスデータを復号化し、データ制御部を介してデータ検証部へ送り、データ検証部は、許可要求データとインデックスデータを比較し、許可要求データが正なものでないかを判断し、正常な要求の場合は、アブリケーションのインストール及びアンインストールの許可通知データを作成し、アブリケーションのインストール及びアンインストール処理を継続する、また、要求データが不正なものであった場合は、アブリケーションデータのインストール及びアンインストール不許可通知である拒否通知データを作成し、出力装置にアブリケーションのインストール及びアンインストールの拒否を示すメッセージを表示し、アブリケーションのインストール及びアンインストール処理を終了させるように構成されている。

【0008】また、第3の発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法は、処理装置は入力装置と出力装置を備え、ファイルの作成及び削除を検知すると、出力装置にキーワード入力画面を表示して、実行者に対して、入力装置よりキーワードを入力させ、マシン名、ユーザ名、パスワード、及びキーワードを含む実行者のデータを暗号化して、ファイルの作成及び削除許可を要求する許可要求データを作成し、また、ファイルの作成及び削除拒否通知データを作成した場合は、出力装置にファイルの作成及び削除の拒否を示すメッセージを表示し、ファイルの作成及び削除処理を終了するように構成されている。

【0009】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

【0010】図1は本発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法の第1の一実施の形態を示す接続系統図である。

【0011】図1を参照すると、本実施の形態は、アブリケーションのインストール及びアンインストールの許可要求が妥当かどうかをセキュリティチェックするサーバ10、サーバ10と同等の機能を持ち、サーバ10がバ10、サーバ10と同等の機能を持ち、サーバ11、アブリケーションのインストール及びアンインストールの許可要求をサーバ10、クライアント20、クライアント21、クライアント22、及び各サーバと各クライアントを結ぶネットワークケーブル30から構成されている。

【0012】図2は本発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法の第1の一実施の形態を示すブロック図である。

【0013】図2を参照すると、サーバ10と、クライアント20、サーバ10の処理に必要なデータを蓄積している記憶装置100からなる。

【0014】サーバ10は、クライアント20から送信された許可要求データを処理するデータ生成部200

と、データ制御部300、データ検証部400を備えている。

【0015】データ生成部200は、データ生成方法の違いにより復号生成部201、暗号生成部202、認証生成部203の3つからなる。復号生成部201は、暗号化されたデータをデータ検証部400で処理できるように復号化する。暗号生成部202は、復号化されたデータを記憶装置100で保管できるように暗号化する。認証生成部203は、復号生成部201で復号化されたデータからデータ検証部400で検証するためのデータを生成する。

【0016】データ制御部300は、クライアント20、データ生成部200、データ制御部300、データ検証部400、記憶装置100を行き交うデータの流れを制御する。

【0017】データ検証部400は、クライアント20より送られた許可要求データが妥当なものであるかを検証する。

【0018】次に、本発明の実施の形態の動作について、図2、図3、図4、及び図5を参照して詳細に説明する。

【0019】図3は本発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法の第1の実施の形態の動作を示す流れ図であり、図4及び図5は本発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法のデータの構成を示す構成図である。

【0020】クライアント20でアブリケーションのインストール及びアンインストールの実行が開始されると、クライアント20のオペレーティングシステムがアブリケーションのインストール及びアンインストール開始状態を検知する(図3のステップA1)。

【0021】次に、クライアント20のオペレーティングシステムでアブリケーションのインストール及びアンインストールを一時停止状態にし、クライアント20で現在操作している実行者のデータ(クライアントマシン名C、ログオンユーザ名D、パスワードE、インストール及びアンインストールするアブリケーション名F、アブリケーションのバージョン情報G)を暗号化して、アブリケーションのインストール及びアンインストール許可を要求する許可要求データB1としてサーバ10へ送信する(ステップA2)。

【0022】サーバ10では、クライアント20から送信された許可要求データB1をデータ制御部300で受信する。データ制御部300では、許可要求データB1をデータ生成部200の復号生成部201へ送る。復号生成部201では、許可要求データB1を復号化してデータ制御部300を介してデータ検証部400へ送る(ステップA3)。

【0023】データ制御部300では、記憶装置100

15  
に格納されているインデックスデータB3を取り出し、データ生成部200の復号生成部201へ送る。復号生成部201では、インデックスデータB3を復号化し、データ制御部300を介してデータ検証部400へ送る。データ検証部400では、許可要求データB1のクライアントマシン名Cがネットワークに存在するもののかをサーバ10のオペレーティングシステムに問い合わせる。存在するならば、許可要求データB1のログオシユーザ名D/パスワードEと、インデックスデータB3のログオンユーザ名D/パスワードEが一致するものかを(図5のサーチ1)する(ステップA4)。

【0024】同じデータが見つかった場合は、データ制御部300がインデックスデータB3のナンバーJをキーとして、記憶装置100に格納されている認証データB4（インデックスデータB3のナンバーJをキーとして昇順に並んでいるデータ）を取り出し（サーチ2）、データ生成部200の復号生成部201へ送る。復号生成部201では、認証データB4を復号化し（ステップA5）、データ制御部300を介してデータ検証部400へ送る。

0へ送る。

【0025】データ検証部400では、許可要求データB1のアプリケーション名F、アプリケーションのバージョン情報Gと、認証データB4のアプリケーション名F、アプリケーションのバージョン情報Gが一致するものを検索(サーチ3)する。

【0026】同じデータが見つかった場合は、アプリケーションのインストール及びアンインストールの実行権限K情報（実行可能または実行不可能と記録されている）が実行可能になっているかをチェック、アプリケーションのインストール及びアンインストール許可の要求を立てるのではないか判断する（ステップA6）。

【0027】不正な要求でない、すなわち正当なアプリケーションのインストール及びアンインストール許可の要求であった場合は、認証データB4をデータ生成200の認証生成部203へ送る。認証生成部203では、認証データB4に正常な操作である旨の履歴L情報を付加する。履歴L情報には、正常操作、クライアントマシン名、ログオンユーザ名、パスワード、操作が行われた時間を含む。また必要であれば実行権限E情報の変更も行う。

【0028】履歴情報と付加する情報は、不正が行われた場合の原因究明に有効な情報となるためである。履歴情報と付加された認証データB4は、データ制御部300を介してデータ生成部200の暗号生成部202へ送り、暗号化する（ステップA7）。

【0029】暗号化された認証データB4はデータ制御部300を介して記憶装置100へ保管される(ステップA8)。

【0030】データ制御部300は認証データが保管された後に、クライアント20へアプリケーションのイン

16  
ストール及びアンインストール許可を通知する許可または  
は坂本通知データB2を送信する(ステップA9)。

【0031】クライアント20ではサーバ10より送られたアプリケーションのインストール及びアンインストール許可を通知する許可または拒否通知データB2を受信し、アプリケーションのインストール及びアンインストールを継続する（ステップA10～A12）。

【0032】以上が正常な操作が行われた際の動作である。  
操作の過失による誤

る。

【0033】次に悪意を持った不正操作や過失による誤操作が行われた際の動作は、ステップA4または、ステップA6で検出される。

【0034】ステップA4では、ネットワークに存在しないクライアントマシン名Cからの不正操作、ログオンユーザ名D/パスワードEが不正であることが検出可能である。

【0035】ステップA6では、個々のアプリケーションに対して不正なインストール及びアンインストールが要求されたかを検出できる。検出されたら認証データB4をデータ生成部200の認証生成部203へ送る。認証生成部203では、認証データB4に不正な操作である旨の履歴情報と付加する。履歴情報には、不正操作の原因究明に必要なデータ（異常操作、クライアントマシン名、ログオンユーザ名、パスワード、操作が行われた時間）を含む。履歴が付加された認証データB4は、データ制御部300を介してデータ生成部200の暗号生成部202へ送り暗号化する（ステップA13）。

3)。  
【0036】暗号化された認証データB4は、データ制御部300を介して記憶装置100へ保管する(ステップA14)。

【0037】データ制御部300は認証データB4データが保管された後に、クライアント20へアプリケーションのインストール及びアンインストール拒否を通知する許可または拒否通知データB2を送信する（ステップA15）。

【0038】クライアント20ではサーバ10より送られたアプリケーションのインストール及びアンインストール拒否を通知する許可または拒否通知データB2を受信(ステップA16)し、アプリケーションのインストール及びアンインストールを中止して終了する。

【0039】本発明の第1の実施の形態では、2つのクライアントの場合は、1台のサーバー、3つのクライアントの場合について説明したが、サーバー、クライアントとともに装置の数に制限はない。

【0040】次に、本発明の第2の実施の形態の動作について、図4、図5、図6、及び図7を参照して詳細に説明する。

【0041】図6は本発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法の第2及び第3の一実施の形態を示すブロック図であ

り、図7は本発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法の第2の実施の形態の動作を示す流れ図である。

【0042】図6を参照すると、本発明の第2の実施の形態は、キーボード等の入力装置13とディスプレイ装置等の出力装置12を備える点、実行者のデータ作成時にデータ入力を必要とする点で異なる。

【0043】本第2の実施の形態の説明では、第1の実施の形態で説明したサーバ/クライアント型の形態ではなく、スタンドアロン型での実施例について説明する。したがって、サーバ10とクライアント20のデータのやり取りであるステップA2からA3、A9からA10、及びA15からA16の処理が不要となり、代わりにデータを作成及び入出力を行うステップC1からC5の処理が追加となる。

【0044】図7のステップA1からA14で示される本第2の実施の形態は、第1の実施の形態のステップA1からA14の動作と同一のため、説明は省略する。なお、本第2の形態では、第1の実施の形態でサーバ10上で行っていたステップA4からA8、ステップA13からA14の処理もスタンドアロン型を構成する処理装置10を含む同一の装置上で行う。

【0045】第1の実施の形態では、クライアント20のオペレーティングシステムが、アプリケーションのインストール及びアンインストールの開始を検知した時点で実行者のデータを暗号化して、許可要求データB1を送信していた。そのため、クライアント20が既に起動済みであれば、クライアント20にログインした本人かどうかを確認する手段がないため、ログインした本人以外が操作した場合でも、インストール及びアンインストールが可能であった。

【0046】本第2の実施の形態では、オペレーティングシステムがアプリケーションのインストール及びアンインストールの開始を検知すると、出力装置12にキーワード入力画面を表示して、実行者に対して、入力装置13よりキーワードHを入力させ（ステップC1）、実行者のデータ（マシン名C、ユーザ名D、パスワードE、キーワードH）を作成して（ステップC2）、アプリケーションのインストール及びアンインストール許可を要求する許可要求データD1として、データ制御部3を介してデータ検証部400へ送る。同時にデータ00を介してデータ検証部400へ送る。同時にデータ制御部300は、記憶装置100に格納されているインデックスデータD2を取り出し、データ生成部200のデータ生成部201へ送る。復号生成部201では、インデックスデータD2を復号化し、データ制御部300を介してデータ検証部400へ送る。データ検証部400では、許可要求データD1とインデックスデータD2を比較し、許可要求データが不正なものでないかを判断する（ステップA6）。

【0047】本第2の実施の形態においては、正常な要

求の場合は、アプリケーションのインストール及びアンインストールの許可または拒否通知データB2を作成し（ステップC3）、アプリケーションのインストール及びアンインストール処理を継続する（ステップA11～A12）。

【0048】一方、要求データが不正なもの（キーワードHが不一致など）であった場合は、アプリケーションのインストール及びアンインストール不許可通知である許可または拒否通知データB2を作成し（ステップC4）、出力装置12にアプリケーションのインストール及びアンインストールの拒否を示すメッセージを表示し（ステップC5）、アプリケーションのインストール及びアンインストール処理を終了させる（ステップA12）。

【0049】次に、本発明の第3の実施の形態の動作について、図8を参照して詳細に説明する。

【0050】図8は本発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法の第3の実施の形態の動作を示す流れ図である。

【0051】図8を参照すると、本発明の第3の実施の形態は、第1、または第2の実施の形態とは、第1及び第2の実施の形態が、アプリケーションのインストール及びアンインストールを対象としていたのに対して、本第3の実施の形態ではファイルの作成及び削除が対象となっている点で異なる。したがって、本発明の第3の実施の形態では、図8のステップA1がファイルの作成及び削除の開始となり、ステップA11がファイルの作成及び削除の実行、ステップA12が、ファイルの作成及び削除の終了となる。

【0052】次に、具体例について説明すると、図6に示すシステムでファイルの作成及び削除を検知すると、出力装置12にキーワード入力画面を表示して、実行者に対して、入力装置13よりキーワードHを入力させ（ステップC1）、実行者のデータ（マシン名C、ユーザ名D、パスワードE、キーワードH）を暗号化して、ファイルの作成及び削除許可を要求する許可要求データD1を作成する（ステップC2）。

【0053】また、ファイルの作成及び削除拒否通知データを作成（ステップC4）した場合は、出力装置12にファイルの作成及び削除の拒否を示すメッセージを表示（ステップC5）し、ファイルの作成及び削除処理を終了する（ステップA12）。

【0054】尚以上のような処理プログラムを記録した記録媒体を有し、コンピュータに実行させることもできる。

【0055】

【発明の効果】以上説明したように、本発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法は、第1の効果は、アプリケーションのインストール及びアンインストールの初期段階、すな

わちファイルの追加または削除が行われる前に、悪意を  
持った不正操作や過失による誤操作を防げることにあ  
る。

【0056】その理由は、アプリケーションのインスト  
ール及びアンインストールの初期段階で不正操作または  
誤操作が検出できるためである。

【0057】第2の効果は、決められたアプリケーショ  
ンのみインストール及びアンインストールを実行するこ  
とが可能になる。

【0058】その理由は、クライアントから許可要求デ  
ータを送信する際に、そのデータにアプリケーション名  
やバージョン情報などを附加しておくことで、記憶装置  
にある認証データのインストール及びアンインストール  
実行権限情報（アプリケーション毎に持つようとする）  
と比較検証することができるためである。

【図面の簡単な説明】

【図1】本発明のセキュリティチェック機能付きインス  
トール及びアンインストール制御装置と方法の第1の一  
実施の形態を示す接続系統図である。

【図2】本発明のセキュリティチェック機能付きインス  
トール及びアンインストール制御装置と方法の第1の一  
実施の形態を示すブロック図である。

【図3】本発明のセキュリティチェック機能付きインス  
トール及びアンインストール制御装置と方法の第1の実  
施の形態の動作を示す流れ図である。

【図4】本発明のセキュリティチェック機能付きインス  
トール及びアンインストール制御装置と方法のデータの

構成を示す構成図である。

【図5】本発明のセキュリティチェック機能付きインス  
トール及びアンインストール制御装置と方法のデータの  
構成を示す構成図である。

【図6】本発明のセキュリティチェック機能付きインス  
トール及びアンインストール制御装置と方法の第2及び  
第3の一実施の形態を示すブロック図である。

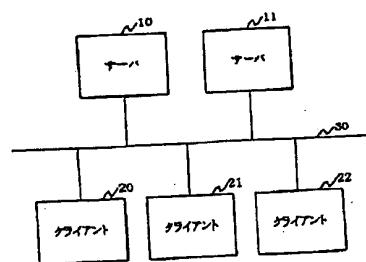
【図7】本発明のセキュリティチェック機能付きインス  
トール及びアンインストール制御装置と方法の第2の実  
施の形態の動作を示す流れ図である。

【図8】本発明のセキュリティチェック機能付きインス  
トール及びアンインストール制御装置と方法の第3の実  
施の形態の動作を示す流れ図である。

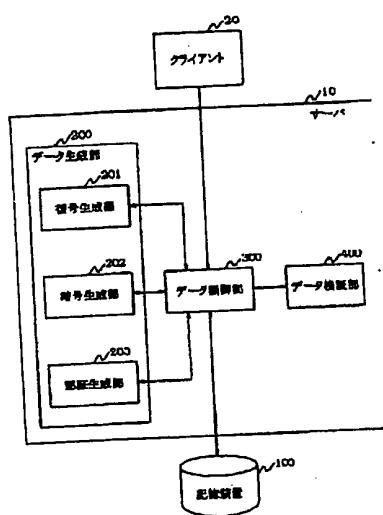
【符号の説明】

1 0	サーバ、処理装置
1 1	サーバ
1 2	出力装置
1 3	入力装置
2 0, 2 1, 2 2	クライアント
3 0	ネットワークケーブル
1 0 0	記憶装置
2 0 0	データ生成部
2 0 1	復号生成部
2 0 2	暗号生成部
2 0 3	認証生成部
3 0 0	データ制御部
4 0 0	データ検証部

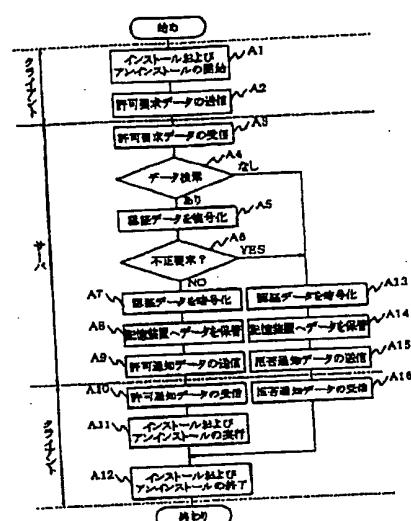
【図1】



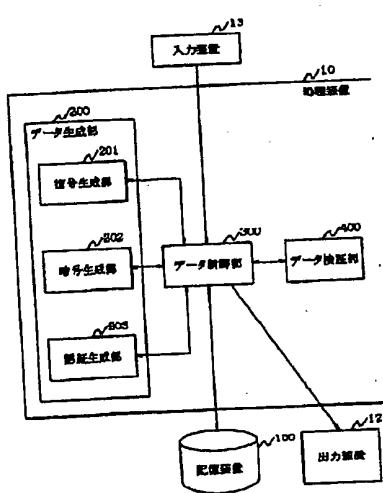
【図2】



【図3】



【図6】



(13)

【図5】

【図4】

(クライアントからサーバへ送られるデータ)

許可要求データB1  
A B C D E F O Etc

許可要求データD1  
A B C D E F O H Etc

(サーバからクライアントへ送られるデータ)

許可応答と拒否通知データB2  
A B I Etc

(サーバの記憶装置に格納されているデータ)

ログインデータB3  
1 B D E Etc

ログアウトデータD2  
J B D E H Etc

属性データB4  
J B F O K L Etc

アソシエーション層に蓄積判定する

【記号の意味】  
A:ヘッダ  
B:番号欄  
C:クライアントマシン名  
D:ログインユーザ名  
E:パスワード  
F:アブリケーション名  
G:バージョン情報  
H:キー/カード  
I:許可/拒否データ  
J:ナンバー  
K:実行権限  
L:履歴  
Etc:将来の拡張用エリア

(データ1)  
ログインユーザ名とパスワードが一致するデータを検索。  
許可要求データB1  
A B C D E F G Etc

ログアウトデータB3  
J B D E Etc

(データ2)  
ナンバーに接続されているデータ検出する属性データB4を検索  
(ログインデータB3の100番台の属性に記載されている。  
属性データB4はナンバーの属性に記載されている。

ログインデータB3  
100 B D E Etc

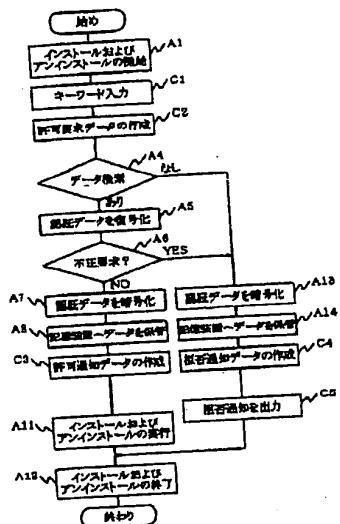
属性データB4  
098 B F G K L Etc  
100 B F O K L Etc  
101 B F O K L Etc

(データ3)  
アプリケーション名とバージョンが一致するデータを検索。  
許可要求データB1  
A B C D E F G Etc

属性データB4  
J B F G K L Etc

【記号の意味】  
A:ヘッダ  
B:番号欄  
C:クライアントマシン名  
D:ログインユーザ名  
E:パスワード  
F:アブリケーション名  
G:バージョン情報  
H:キー/カード  
I:許可/拒否データ  
J:ナンバー  
K:実行権限  
L:履歴  
Etc:将来の拡張用エリア

[圖 7]



[図8]

